Docket No.: 10016591-1
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Richard P. Tarquini et al.

Application No.: 10/001,446

Confirmation No.: 2400

Filed: October 31, 2001

Art Unit: 2132

For: NETWORK, METHOD AND COMPUTER
READABLE MEDIUM FOR DISTRIBUTING
SECURITY UPDATES TO SELECT NODES
ON A NETWORK

Examiner: L. L. Lashley

REPLY BRIEF

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

As required under § 41.41(a)(1), this Reply Brief is filed within two months of the

Examiner's Answer dated September 27, 2006, and is in furtherance of the Appeal Brief filed on

July 11, 2006.

No fee is required for this REPLY BRIEF.

This brief contains items under the following headings pursuant to M.P.E.P. § 1208:

I.	Status of Claims
II.	Grounds of Rejection to be Reviewed on Appeal
III.	Argument
IV.	Conclusion
V.	Corrected Claims Appendix

25712057.1

I.   STATUS OF CLAIMS

The status of claims remains as identified in the Appeal Brief submitted July 11, 2006, wherein claims 1-10 are on appeal.

II.   GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The grounds of rejection to be reviewed on appeal remain the same as identified in the Appeal Brief submitted July 11, 2006.

III.   ARGUMENT

Appellant respectfully traverses the outstanding claim rejections and requests that the Board reverse those rejections in light of the remarks presented below. Appellant hereby reasserts those arguments that are presented for the separately argued claims in the Appeal Brief. For brevity, however, Appellant does not repeat those arguments herein and submits the following supplemental remarks in reply to the Examiner's Answer.

A. Rejections under 35 U.S.C. §102 over *Holloway*

Claims 1-10 stand rejected under 35 U.S.C. § 102 as being anticipated by *Holloway*. In order to anticipate a claim under 35 U.S.C. § 102, a single reference must teach each and every element of the claim. *See Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631 (Fed. Cir. 1987). As discussed below, Appellant respectfully submits that *Holloway* fails to teach each and every element of the claims, and respectfully requests that the Board overturn these rejections.

1.   Independent Claim 1 and Dependent Claims 2-7

Claim 1 recites, in part, "a plurality of nodes connected to the network medium and running an instance of an intrusion protection system application, at least one of the nodes having an identification assigned thereto based on a logical assignment grouping one or more of the plurality of nodes, each node sharing an identification being commonly vulnerable to at least

one network exploit." The Examiner appears to rely upon *Holloway*'s managed hub as meeting the claimed nodes. Examiner's Answer, page 3. According to *Holloway*,

> the managed hub determines the interconnect devices in the campus network that are capable of supporting the LAN security feature. The managed hub periodically sends a discovery frame to the LAN security feature group address. The managed hub then uses the responses to build and maintain a table of interconnect devices in the network that support the security feature.

Holloway, column 3, lines 26-32. *Holloway*'s managed hubs themselves are <u>not</u> grouped together. Rather, *Holloway* merely discloses that its managed hubs may assemble a list of interconnect devices that support a particular security feature. *Id.*

Insofar as the Examiner may also be relying upon *Holloway*'s interconnect devices as meeting the claimed "nodes", Appellant notes that *Holloway* does not teach that such interconnect devices "[run] an instance of an intrusion protection system application," as recited in claim 1. Moreover, while *Holloway*'s interconnect devices may be grouped according to their ability to support a security feature, they are not grouped according to a common vulnerability to a network exploit, as also recited in claim 1. Thus, Holloway fails to teach all elements of the claim arranged as required by the claim.

In response to the above arguments, the Examiner's Answer asserts on page 6 thereof:

> [t]he Examiner believes the LAN security feature group address is the vulnerability by which the nodes are grouped. Further, responses received from the managed hubs and maintaining a list of interconnected devices that support the LAN security feature signify that devices are in communication and are aware of other authorized/valid nodes meeting the limitation of the claim (see column 3, lines 25-32 column 5, lines 17-22; column 7, lines 33-48). Appellant is essentially arguing that the references fail to show limitations not present in the rejected claim.

First, Appellant is not arguing limitations that are not present in the rejected claim. Specifically, claim 1 recites "a plurality of nodes connected to the network medium and running an instance of an intrusion protection system application, <u>at least one of the nodes having an</u> <u>identification assigned thereto based on a logical assignment grouping one or more of the</u>

plurality of nodes, each node sharing an identification being commonly vulnerable to at least one network exploit" (emphasis added). *Holloway* simply provides no teaching of assigning an identification to nodes where nodes that share an identification are commonly vulnerable to at least one network exploit. *Holloway* provides no teaching of determining those nodes that are commonly vulnerable to a network exploit, and thus, *Holloway* provides no teaching of assigning an identification to nodes such that nodes that share an identification are commonly vulnerable to at least one network exploit as expressly recited by claim 1.

The Examiner asserts on page 3 of the Answer that "the MAC address is the ID and each node has an authorized address". However, the MAC address is not taught as being assigned to nodes that are commonly vulnerable to a network exploit. Rather, as is well-known, in a local area network (LAN) or other network, the MAC (Media Access Control) address is a computer's unique hardware number. When connected to the Internet, a correspondence table relates a computer's IP address to the computer's physical (MAC) address on the LAN. Thus, the MAC address provides an identification of a computer, but *Holloway* does not teach that nodes sharing such an identification (i.e., sharing a MAC address) are commonly vulnerable to at least one network exploit. For instance, *Holloway* does not teach that nodes assigned the same MAC address are commonly vulnerable to at least one network exploit. Assuming for instance, that multiple nodes can be assigned a common MAC address, the nodes might have different network exploit vulnerabilities based on their different configurations for providing different services, for example, *see e.g.*, page 18, line 18 – page 19, line 31 of the present application.

Accordingly, for the reasons discussed above, *Holloway* fails to teach all elements of claim 1. Therefore, Appellant respectfully requests that the Board overturn the rejection of record with respect to claim 1.

Dependent claims 2-7 depend either directly or indirectly from claim 1, thus inheriting all of the limitations of that independent claim. As noted above, *Holloway* does not teach every element of independent claim 1. Consequently, *Holloway* also fails to teach every element of dependent claims 2-7. Therefore, Appellant respectfully requests that the Board overturn the rejection of record with respect to claims 2-7.

2.   <u>Dependent Claim 8</u>

Dependent claim 8 depends from claim 1, thus inheriting all of the limitations of that independent claim. As noted above, *Holloway* does not teach every element of independent claim 1. Consequently, *Holloway* also fails to teach every element of dependent claim 8. Moreover, claim 8 recites additional limitations not taught by *Holloway*.

For example, claim 8 recites "a network-based intrusion protection system appliance dedicated to filtering inbound and outbound data frames transmitted across the network medium." The Examiner relies upon *Holloway*'s network management station as meeting the claimed network-based intrusion protection system appliance. Examiner's Answer, page 5. However, there is no indication that *Holloway*'s network management station is an intrusion protection appliance. Furthermore, column 18, lines 10-13 of *Holloway* (cited by the Examiner in support of this rejection, *see* page 5 of the Examiner's Answer) merely discloses transmitting and receiving a discovery request frame in order to build an interconnect device list. Appellant respectfully points out that such steps are performed by a managed hub, and not by the network management station. *See e.g.*, *Holloway*, column 3, lines 32-36.

Accordingly, for the reasons discussed above, *Holloway* fails to teach all elements of claim 8. Therefore, Appellant respectfully requests that the Board overturn the rejection of record with respect to claim 8.

3.   <u>Dependent Claim 9</u>

Dependent claim 9 depends indirectly from claim 1, thus inheriting all of the limitations of that independent claim. As noted above, *Holloway* does not teach every element of independent claim 1. Consequently, *Holloway* also fails to teach every element of dependent claim 9. Moreover, claim 9 recites additional limitations not taught by *Holloway*.

For example, claim 9 recites that "the network-based intrusion protection system appliance interfaces with the network medium via a network interface card operating in promiscuous mode." As previously noted, *Holloway* does not teach, or even suggest, an intrusion protection system appliance, much less an intrusion protection system appliance that

interfaces with the network medium via a network interface card operating in promiscuous mode, as recited in claim 9. There is no mention identified in *Holloway* of such a promiscuous mode.

Accordingly, for the reasons discussed above, *Holloway* fails to teach all elements of claim 9. Therefore, Appellant respectfully requests that the Board overturn the rejection of record with respect to claim 9.

4.   Dependent Claim 10

Dependent claim 10 depends indirectly from claim 1, thus inheriting all of the limitations of that independent claim. As noted above, *Holloway* does not teach every element of independent claim 1. Consequently, *Holloway* also fails to teach every element of dependent claim 10. Moreover, claim 10 recites additional limitations not taught by *Holloway*.

For example, claim 10 recites that "the network-based intrusion protection system appliance shares [an] identification." Applicant points out that claim 1, from which claim 10 depends, provides that the identification is assigned based on a logical assignment grouping one or more of the plurality of nodes, each node sharing an identification being commonly vulnerable to at least one network exploit. As previously noted, *Holloway* does not teach an intrusion protection system appliance, much less an intrusion protection system appliance that shares an identification assigned based on a logical assignment grouping one or more of the plurality of nodes, each node sharing an identification being commonly vulnerable to at least one network exploit, as recited in claim 10.

Accordingly, for the reasons discussed above, *Holloway* fails to teach all elements of claim 10. Therefore, Appellant respectfully requests that the Board overturn the rejection of record with respect to claim 10.

IV.   CONCLUSION

Appellant respectfully requests that the Board overturn the rejections of pending claims 1-10 for the above reasons. Attached hereto is a copy of the claims appendix, in which the minor typographical error in claim 6 (as noted in the Examiner Answer, page 2) is corrected.

Respectfully submitted,

By: _____
Jody C. Bishop
Attorney/Agent for Applicant(s)
Reg. No. 44,034
Date: November 20, 2006
Telephone No. (214) 855-8007

V.   CORRECTED CLAIMS APPENDIX

Claims Involved in the Appeal of Application Serial No. 10/001,446:

1.   A network having an intrusion protection system, comprising:

a network medium;

a management node connected to the network medium and running an intrusion prevention system management application; and

a plurality of nodes connected to the network medium and running an instance of an intrusion protection system application, at least one of the nodes having an identification assigned thereto based on a logical assignment grouping one or more of the plurality of nodes, each node sharing an identification being commonly vulnerable to at least one network exploit.

2.   The network according to claim 1 wherein the management node is operable to originate a security update that is transmitted to each node sharing the identification, any remaining nodes not sharing the identification being excluded from receiving the update.

3.   The network according to claim 1 wherein a plurality of identifications are respectively assigned to one or more of the plurality of nodes.

4.   The network according to claim 1 wherein the identification is an Internet Protocol multicast group identification.

5.   The network according to claim 2 further comprising:

a plurality of network mediums; and

at least one router, the management node and the plurality of nodes each respectively connected to one of the plurality of network mediums in the network, the router disposed intermediate the plurality of network mediums and operable to forward the security update from the network medium having the management node connected thereto to any nodes connected to the remaining network mediums and sharing the identification.

6.   The network according to claim 5 wherein the router determines whether any of the plurality of nodes connected to the remaining network mediums share the identification through implementation of the Internet group management protocol.

7.   The network according to claim 1 wherein the network medium is an Ethernet.

8.   The network according to claim 1 further comprising a network-based intrusion protection system appliance dedicated to filtering inbound and outbound data frames transmitted across the network medium.

9.   The network according to claim 8 wherein the network-based intrusion protection system appliance interfaces with the network medium via a network interface card operating in promiscuous mode.

10.   The network according to claim 8 wherein the network-based intrusion protection system appliance shares the identification.